

1 **In the Claims**

2  
3 1. (Currently Amended) A method comprising:

4 creating a data structure including a plurality of user id-user key pairs, each  
5 user id-user key pair comprising a user id associated with one of a plurality of  
6 users and a user key comprising a master key and a keyed-hash message  
7 authentication code encrypted using a password associated with the one of the  
8 plurality of users; and

9 delivering the data structure to one or more of the plurality of users.

10  
11 2. (Original) A method as recited in claim 1, wherein the act of  
12 delivering comprises delivering the data structure to each of the plurality of users.

13  
14 3. (Original) A method as recited in claim 1, wherein each master key  
15 is encrypted using a hash of the password associated with the one of the plurality  
16 of users.

17  
18 4. (Original) A method as recited in claim 1, wherein each master key  
19 is encrypted using a one-way hash of the password associated with the one of the  
20 plurality of users.

21  
22 5. (Original) A method as recited in claim 1, wherein each master key  
23 is encrypted using a cryptographic hash of the password associated with the one of  
24 the plurality of users.  
25

6. (Original) A method as recited in claim 1, wherein each user key has an integrity verification feature associated therewith.

7. (Original) A method as recited in claim 1, wherein each master key has an integrity verification feature associated therewith.

8. (Currently Amended) A method as recited in claim 1, wherein each master key and each ~~master~~-user key has an integrity verification feature associated therewith.

9. (Original) A method as recited in claim 1, wherein each user key includes a checksum.

10. (Cancel)

11. (Original) A method as recited in claim 1, further comprising:  
transforming data using the master key.

12. (Original) A method as recited in claim 1, further comprising:  
storing data transformed using the master key; and  
controlling access by the plurality of users to the transformed data.

13. (Original) A method as recited in claim 1, further comprising:  
storing data transformed using the master key;  
receiving a user id and user password from one of the plurality of users; and  
controlling access to the transformed data by the one of the plurality of  
users based on the received user id and user password.

14. (Original) A method as recited in claim 1, further comprising:  
storing data transformed using the master key;  
receiving a user id and user password from one of the plurality of users; and  
accessing the transformed data using the received user id and user  
password.

15. (Currently Amended) A method as recited in claim 1, further  
comprising:  
storing data transformed using the master key;  
receiving a user id and user password from one of the plurality of users;  
selecting a user key from the data structure based on the received user id;  
decrypting the selected user id-key using the received password to  
reproduce the master key; and  
using the master key to access the data.

1 16. (Currently Amended) A method as recited in claim 1, further  
2 comprising:

3 storing data watermarked using the master key;  
4 receiving a user id and user password from one of the plurality of users; and  
5 selecting a user key from the data structure based on the received user id;  
6 hashing the received password to produce a hash value;  
7 decrypting the selected user id-key using the hash value to reproduce the  
8 master key; and  
9 using the master key to access the watermarked data.

10  
11 17. (Withdrawn) A method comprising:

12 retrieving a user key associated with a first user of a plurality of users from  
13 a data structure comprising a plurality of user keys, each user key comprising a  
14 master key encrypted using a password associated with a unique one of the  
15 plurality of users;

16 decrypting the retrieved user key using a password associated with the first  
17 user to produce a master key; and

18 accessing data using the master key.

19  
20 18. (Withdrawn) A method as recited in claim 17, wherein the user key  
21 is retrieved using a user id associated with the first user.

1           19. (Withdrawn) A method as recited in claim 17, wherein the data  
2 structure comprises a plurality of user id-user key pairs, each user id-user key pair  
3 comprising a user id associated with one of a plurality of users and a user key  
4 associated with the one of the plurality of users.

5  
6           20. (Withdrawn) A method as recited in claim 17, wherein the data  
7 structure comprises a plurality of user id-user key pairs, each user id-user key pair  
8 comprising a user id associated with one of a plurality of users and a user key  
9 associated with the one of the plurality of users, and wherein the user key is  
10 retrieved using a user id associated with the first user.

11  
12           21. (Withdrawn) A method as recited in claim 17, wherein the act of  
13 decrypting the user key comprises decrypting the user key using a hash of the  
14 password associated with the first user.

15  
16           22. (Withdrawn) A method as recited in claim 17, wherein the act of  
17 decrypting the retrieved user key comprises:

18           hashing the password associated with the first user to produce a hash value;  
19 and  
20           using the hash value as a decryption key to decrypt the user key.

1  
2 23. (Withdrawn) A method as recited in claim 17, wherein the act of  
3 decrypting the retrieved user key comprises:

4 hashing the password associated with the first user using a one-way hash  
5 function; and

6 using the result of the one-way hash function as a decryption key to decrypt  
7 the user key.

8  
9 24. (Withdrawn) A method as recited in claim 17, wherein the act of  
10 decrypting the retrieved user key comprises:

11 hashing the password associated with the first user using a cryptographic  
12 hash function; and

13 using the result of the cryptographic hash function as a decryption key to  
14 decrypt the user key.

15  
16 25. (Withdrawn) A method as recited in claim 17, wherein each of the  
17 plurality of user keys includes a data verification feature.

18  
19 26. (Withdrawn) A method as recited in claim 17, wherein each of the  
20 plurality of master keys includes a data verification feature.

21  
22 27. (Withdrawn) A method as recited in claim 17, further comprising:  
23 verifying the integrity of the retrieved user key.  
24  
25

1           28. (Withdrawn) A method as recited in claim 17, wherein the retrieved  
2 user key includes an integrity verification feature and wherein the method further  
3 comprises verifying the integrity of the retrieved user key using the integrity  
4 verification feature.

5  
6           29. (Withdrawn) A method as recited in claim 17, wherein the retrieved  
7 user key includes a checksum and wherein the method further comprises verifying  
8 the integrity of the retrieved user key using the checksum.

9  
10          30. (Withdrawn) A method as recited in claim 17, wherein the retrieved  
11 user key includes a message authentication code and wherein the method further  
12 comprises verifying the integrity of the retrieved user key using the message  
13 authentication code.

14  
15          31. (Withdrawn) A method as recited in claim 17, wherein the retrieved  
16 user key includes a keyed-hash message authentication code and wherein the  
17 method further comprises verifying the integrity of the retrieved user key using the  
18 keyed-hash message authentication code.

32. (Currently Amended) A computer readable medium having stored thereon a data structure comprising:

a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key and a keyed-hash message authentication code encrypted using a password associated with the one of the plurality of users.

33. (Original) A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a hash of the password associated with the one of the plurality of users.

34. (Original) A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a one-way hash of the password associated with the one of the plurality of users.

35. (Original) A computer readable medium as recited in claim 32, wherein each user key comprises a master key encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

36. (Original) A computer readable medium as recited in claim 32, wherein each user key includes an integrity verification feature.

37. (Original) A computer readable medium as recited in claim 32, wherein each master key includes an integrity verification feature.



1  
2 38. (Original) A computer readable medium as recited in claim 32,  
3 wherein each user key includes a checksum.

4  
5 39. (Cancel)

6  
7 40. (Withdrawn) A system comprising:  
8 a hashing module operable to hash each of a plurality of user passwords to  
9 produce a plurality of hash values;

10 an encryption module operable to create a plurality of user keys, each user  
11 key comprising a master key encrypted using one of the hash values as an  
12 encryption key; and

13 a data structure creation module operable to associate each of the user keys  
14 with a user id in a data structure.

15  
16 41. (Withdrawn) A system as defined in claim 40, wherein the hashing  
17 module produces the hash values using a one-way hashing function.

18  
19 42. (Withdrawn) A system as defined in claim 40, wherein the hashing  
20 module produces the hash values using a cryptographic hashing function.

21  
22 43. (Withdrawn) A system as defined in claim 40, wherein the data  
23 structure creation module associates each user key with a user id in a user id-user  
24 key pair, and wherein each user id-user key pair is associated with a single user.

1  
2 44. (Withdrawn) A system as defined in claim 40, wherein the  
3 encryption module includes an integrity verification feature in each user key.  
4

5 45. (Withdrawn) A system as defined in claim 40, wherein the  
6 encryption module includes a checksum in each user key.  
7

8 46. (Withdrawn) A system as defined in claim 40, wherein the  
9 encryption module includes a message authentication code in each user key.  
10

11 47. (Withdrawn) A system as defined in claim 40, wherein the  
12 encryption module includes a keyed-hash message authentication code in each  
13 user key.  
14

15 48. (Withdrawn) A system comprising:  
16 a user key data structure including plurality of user id-user key pairs, each  
17 user key pair including a user key and a user id associated with one of a plurality  
18 of users, each user key comprising an encrypted version of a common master key;  
19 a master key decryption module operable to select a user key from the user  
20 key data structure based on a user id received from one of the plurality of users  
21 and to decrypt the selected user key using a password received from the one of the  
22 plurality of users.  
23  
24  
25

1           49. (Withdrawn) A system as recited in claim 48, further comprising a  
2 data decryption module operable to decrypt data encrypted using the master key as  
3 an encryption key.

4  
5           50. (Withdrawn) A system as recited in claims 48, further comprising an  
6 error handler module operable to indicate to the one of the plurality when an error  
7 occurs in decrypting the user key.

8  
9           51. (Withdrawn) A system as recited in claims 48, wherein the master  
10 key decryption module comprises:

11           a hashing module operable to hash a password received from the one of the  
12 plurality of users to produce a hash value; and

13           a user key decryption module operable to select a user key from the user  
14 key data structure based on a user id received from one of the plurality of users  
15 and to decrypt the selected user key using the hash value as a decryption key.

16  
17           52. (Withdrawn) A system as recited in claims 48, wherein the master  
18 key decryption module comprises:

19           a hashing module operable to hash a password received from the one of the  
20 plurality of users using a one-way hashing function to produce a hash value; and

21           a user key decryption module operable to select a user key from the user  
22 key data structure based on a user id received from one of the plurality of users  
23 and to decrypt the selected user key using the hash value as a decryption key.  
24  
25

1           53. (Withdrawn) A system as recited in claim 48, wherein the master  
2 key decryption module comprises:

3           a hashing module operable to hash a password received from the one of the  
4 plurality of users using a cryptographic hashing function to produce a hash value;  
5 and

6           a user key decryption module operable to select a user key from the user  
7 key data structure based on a user id received from one of the plurality of users  
8 and to decrypt the selected user key using the hash value as a decryption key.

9  
10           54. (Withdrawn) A system as recited in claims 48, wherein the master  
11 key decryption module comprises:

12           a hashing module operable to hash a password received from the one of the  
13 plurality of users to produce a hash value; and

14           a user key decryption and integrity module operable to select a user key  
15 from the user key data structure based on a user id received from one of the  
16 plurality of users, to confirm the integrity of the selected user id, and to decrypt  
17 the selected user key using the hash value as a decryption key.

1           55. (Withdrawn) A system as recited in claims 48, wherein each user  
2 key in the user key data structure includes an integrity verification feature, and  
3 wherein the master key decryption module comprises:

4           a hashing module operable to hash a password received from the one of the  
5 plurality of users to produce a hash value; and

6           a user key decryption and integrity module operable to select a user key  
7 from the user key data structure based on a user id received from one of the  
8 plurality of users, to confirm the integrity of the selected user id using the integrity  
9 verification feature included in the user key, and to decrypt the selected user key  
10 using the hash value as a decryption key.

11  
12           56. (Currently Amended) A system comprising:

13           means for producing a user key associated with each of a plurality users,  
14 each user key comprising a master key and a keyed-hash message authentication  
15 code encrypted using a password of the one of the plurality of users associated  
16 with the user key; and

17           means for associating each of the user keys with a user id of the one of the  
18 plurality of users associated with the user key in a data structure.

1 57. (Currently Amended) A computer-readable medium having stored  
2 thereon computer executable instructions for performing acts of:

3 creating a data structure including a plurality of user id-user key pairs, each  
4 user id-user key pair comprising a user id associated with one of a plurality of  
5 users and a user key comprising a master key and a keyed-hash message  
6 authentication code encrypted using a password associated with the one of the  
7 plurality of users.

8  
9 58. (Original) A computer-readable medium as recited in claim 57  
10 having further computer executable instructions for performing acts of:  
11 delivering the data structure to one or more of the plurality of users.

12  
13 59. (Cancel)

14  
15 60. (Original) A computer-readable medium as recited in claim 57,  
16 wherein each master key is encrypted using a hash of the password associated with  
17 the one of the plurality of users.

18  
19 61. (Original) A computer-readable medium as recited in claim 57,  
20 wherein each master key is encrypted using a one-way hash of the password  
21 associated with the one of the plurality of users.

1           62. (Original) A computer-readable medium as recited in claim 57,  
2 wherein each master key is encrypted using a cryptographic hash of the password  
3 associated with the one of the plurality of users.

4  
5           63. (Original) A computer-readable medium as recited in claim 57,  
6 wherein each user key has an integrity verification feature associated therewith.

7  
8           64. (Original) A computer-readable medium as recited in claim 57,  
9 wherein each user key includes a checksum.

10  
11           65. (Original) A computer-readable medium as recited in claim 57,  
12 wherein each user key includes a keyed-hash message authentication code.

13  
14           66. (Original) A computer-readable medium as recited in claim 57  
15 having further computer executable instructions for performing acts of:  
16 transforming data using the master key.

17  
18           67. (Original) A computer-readable medium as recited in claim 57  
19 having further computer executable instructions for performing acts of:  
20 storing data transformed using the master key; and  
21 controlling access by the plurality of users to the transformed data.

22  
23           68. (Original) A computer-readable medium as recited in claim 57  
24 having further computer executable instructions for performing acts of:  
25

1 storing data transformed using the master key;  
2 receiving a user id and user password from one of the plurality of users; and  
3 controlling access to the transformed data by the one of the plurality of  
4 users based on the received user id and user password.

5  
6 69. (Original) A computer-readable medium as recited in claim 57  
7 having further computer executable instructions for performing acts of:  
8 storing data encrypted using the master key;  
9 receiving a user id and user password from one of the plurality of users; and  
10 accessing the transformed data using the received user id and user  
11 password.

12  
13 70. (Currently Amended) A computer-readable medium as recited in  
14 claim 57 having further computer executable instructions for performing acts of:  
15 storing data encrypted using the master key;  
16 receiving a user id and user password from one of the plurality of users;  
17 selecting a user key from the data structure based on the received user id;  
18 decrypting the selected user id-key using the received password to  
19 reproduce the master key; and  
20 using the master key to decrypt the data.  
21  
22  
23  
24  
25



1           71. (Currently Amended) A computer-readable medium as recited in  
2 claim 57 having further computer executable instructions for performing acts of:  
3           storing data watermarked using the master key;  
4           receiving a user id and user password from one of the plurality of users; and  
5           selecting a user key from the data structure based on the received user id;  
6           hashing the received password to produce a hash value;  
7           decrypting the selected user id-key using the hash value to reproduce the  
8 master key; and  
9           using the master key to access the watermarked data.

10           72. (Withdrawn) A computer-readable medium having stored thereon  
11 computer executable instructions for performing acts of:  
12           retrieving a user key associated with a first user of a plurality of users from  
13 a data structure comprising a plurality of user keys, each user key comprising a  
14 master key encrypted using a password associated with a unique one of the  
15 plurality of users;  
16           decrypting the retrieved user key using a password associated with the first  
17 user to produce a master key; and  
18           accessing data using the master key.

19           73. (Withdrawn) A computer-readable medium as recited in claim 72,  
20 wherein the user key is retrieved using a user id associated with the first user.  
21  
22  
23  
24  
25

1           74. (Withdrawn) A computer-readable medium as recited in claim 72,  
2 wherein the data structure comprises a plurality of user id-user key pairs, each user  
3 id-user key pair comprising a user id associated with one of a plurality of users  
4 and a user key associated with the one of the plurality of users.

5  
6           75. (Withdrawn) A computer-readable medium as recited in claim 72,  
7 wherein the data structure comprises a plurality of user id-user key pairs, each user  
8 id-user key pair comprising a user id associated with one of a plurality of users  
9 and a user key associated with the one of the plurality of users, and wherein the  
10 user key is retrieved using a user id associated with the first user.

11  
12           76. (Withdrawn) A computer-readable medium as recited in claim 72,  
13 wherein the act of decrypting the user key comprises decrypting the user key using  
14 a hash of the password associated with the first user.

15  
16           77. (Withdrawn) A computer-readable medium as recited in claim 72,  
17 wherein the act of decrypting the retrieved user key comprises:  
18           hashing the password associated with the first user to produce a hash value;  
19           and  
20           using the hash value as a decryption key to decrypt the user key.

1  
2 78. (Withdrawn) A computer-readable medium as recited in claim 72,  
3 wherein the act of decrypting the retrieved user key comprises:

4 hashing the password associated with the first user using a one-way hash  
5 function; and

6 using the result of the one-way hash function as a decryption key to decrypt  
7 the user key.

8  
9 79. (Withdrawn) A computer-readable medium as recited in claim 72,  
10 wherein the act of decrypting the retrieved user key comprises:

11 hashing the password associated with the first user using a cryptographic  
12 hash function; and

13 using the result of the cryptographic hash function as a decryption key to  
14 decrypt the user key.

15  
16 80. (Withdrawn) A computer-readable medium as recited in claim 72,  
17 wherein each of the plurality of user key includes a data verification feature.

18  
19 81. (Withdrawn) A computer-readable medium as recited in claim 72  
20 having further computer executable instructions for performing acts of:

21 verifying the integrity of the retrieved user key.  
22  
23  
24  
25

1           82. (Withdrawn) A computer-readable medium as recited in claim 72,  
2 wherein the retrieved user key includes an integrity verification feature and  
3 wherein the method further comprises verifying the integrity of the retrieved user  
4 key using the integrity verification feature.

5  
6           83. (Withdrawn) A computer-readable medium as recited in claim 72,  
7 wherein the retrieved user key includes a checksum and wherein the method  
8 further comprises verifying the integrity of the retrieved user key using the  
9 checksum.

10  
11           84. (Withdrawn) A computer-readable medium as recited in claim 72,  
12 wherein the retrieved user key includes a message authentication code and  
13 wherein the method further comprises verifying the integrity of the retrieved user  
14 key using the message authentication code.

15  
16           85. (Withdrawn) A computer-readable medium as recited in claim 72,  
17 wherein the retrieved user key includes a keyed-hash message authentication code  
18 and wherein the method further comprises verifying the integrity of the retrieved  
19 user key using the keyed-hash message authentication code.  
20  
21  
22  
23  
24  
25